

CLAIMS

1. A subscriber identification module for providing local authentication of a subscriber in a communication system, comprising:

a memory; and

a processor configured to implement a set of instructions stored in the memory, the set of instructions for:

generating a plurality of keys in response to a received challenge;

generating an authentication signal based on a received signal and a first key from the plurality of keys, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit; and

transmitting the authentication signal to the communications system via the communications unit.

2. The processor of 1, wherein the authentication signal is generated by a hash function.

3. The processor of 2, wherein the hash function is the Secure Hash Algorithm (SHA-1).

4. The processor of 1, wherein the authentication signal is generated by an encryption algorithm.

5. The processor of 4, wherein the encryption algorithm is the Data Encryption Standard (DES).

- 09755660-010501 4

one secret key from the plurality of keys is not delivered to the communications unit; and

a signature generator for generating an authorization signal from both the at least one secret key and from an authorization message, wherein the authorization message is generated by the communications unit using the at least one communication key.

11. The subscriber identification module of Claim 10, wherein the subscriber identification module is configured to be inserted into the communications unit.

12. The subscriber identification module of Claim 10, wherein the signature generator generates the authorization signal by using a hash function.

13. The subscriber identification module of Claim 10, wherein the signature generator generates the authorization signal by using the Data Encryption Standard (DES).

14. The subscriber identification module of Claim 10, wherein the at least one communication key comprises an integrity key.

15. The subscriber identification module of 12, wherein the hash function is SHA-1.

16. A method for providing authentication of a subscriber using a subscriber identification device, comprising:

generating a plurality of keys;

transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys;

09755660.010501

generating a signature at the communications device using both the at
least one key transmitted to the communications device and a transmission
message;

transmitting the signature to the subscriber identification device;

receiving the signature at the subscriber identification device;

generating a primary signature from the received signature; and

conveying the primary signature to a communications system.

17. The method of Claim 16, wherein the generating of the signature signal is
performed using a nonreversible operation.

18. The method of Claim 16, wherein the generating of the signature signal is
performed using DES.

19. The method of Claim 16, wherein the generating of the signature signal is
performed using a hash function.

20. The method of Claim 19, wherein the hash function is SHA-1.

21. A method for providing authentication of a subscriber using a subscriber
identification device, comprising:

generating a plurality of keys;

transmitting at least one key from the plurality of keys to a
communications device communicatively coupled to the subscriber identification
device and holding private at least one key from the plurality of keys;

assigning a weight to the transmission message at the communications
device in accordance with a relative importance of the transmission message;

generating a signature at the communications device using both the at
least one key transmitted to the communications device and the transmission
message;

09755660.010501

